Andrzej Koziara
Oddział Obsługi Informatycznej Bibliotek Uniwersytetu Śląskiego

Prace nad wdrożeniem procedur zabezpieczających przestrzeganie Ustawy o Ochronie Danych Osobowych oraz związanych z nią rozporządzeń wykonawczych

Pierwszego maja 2005 r. minął rok od wejścia Polski do Unii Europejskiej. Data to historyczna nie tylko ze względów politycznych, ale również i prawnych. Dzień ten stał się granicą, kiedy wiele uregulowań prawnych zostało zsynchronizowanych z prawem europejskim.

Prace nad synchronizacją prawa polskiego z uregulowaniami europejskimi przebiegały niestety w trybie bardzo przyspieszonym i zmusiły nas praktycznie do natychmiastowych, sprawnych działań normalizujących nasz styl pracy.

Stało się to tym bardziej ważne, że życie codzienne przynosi bardzo dużo informacji o tym, że wiele organizacji, zarówno komercyjnych, jak i tych, które nie prowadzą takiej działalności, poświęca bardzo mało uwagi zagadnieniom ochrony informacji przez nie gromadzonych. Zjawiska te występują oczywiście z różnym natężeniem na całym świecie, lecz świadomość zagrożeń jest ta sama tzn. bardzo niska. Oczywiście w zależności od kraju i od rodzaju firmy, sposoby ataków w celu uzyskania nieuprawnionego dostępu do danych są różne, ale jeśli są w ogóle podejmowane, to kończą się z reguły powodzeniem.

Jak wykazuje doświadczenie, dla intruzów z zewnątrz łakomym kąskiem są nie tylko dane osobowe, lecz również wszystkie informacje, za które mogą uzyskać odpowiednie wynagrodzenie. Pozyskane tą drogą informacje, z pozoru bardzo błahe, mogą utrudniać późniejszą, sprawną pracę firmy.

Unormowania prawne służące ochronie danych osobowych powinny stać się inspiracją do podjęcia działań porządkujących zestaw procedur, opisujących czynności związane z zarządzaniem biblioteką. Pozwalają również na optymalizację procesów zachodzących w analizowanej instytucji, prowadząc do powiększenia efektów jej pracy przy zachowaniu niezmienionego poziomu kosztów.

Dla zrozumienia sposobu, w jaki winniśmy organizować prace nad wdrożeniem systemów bezpieczeństwa należy zauważyć, że wszystkie działania podejmowane w celu zwiększenia poziomu bezpieczeństwa systemów informatycznych mają swoje źródło w przepisach prawa (krajowego, regionalnego lub firmowego) natomiast realizowane są w sferze organizacyjnej i technicznej. Dla osiągnięcia zamierzonych efektów działania podejmowane przez jednostki podrzędne muszą wynikać z działań jednostek nadrzędnych.

Wszystkie czynności podejmowane przez jednostki gromadzące dane osobowe (w szczególności te, które zgłosiły swoje zbiory danych osobowych do Głównego Inspektora Ochrony Danych Osobowych) muszą być zgodne z zasadami określonymi w *Ustawie o ochronie danych osobowych* z dnia 29 sierpnia 1997 roku, z późniejszymi zmianami opublikowanej w postaci jednolitego tekstu w Dzienniku Ustaw 2002 r. Nr 101

poz. 926. Integralnymi składnikami tej ustawy są wydane rok temu rozporządzenia Ministra Spraw Wewnętrznych i Administracji wynikające z art. 39a ustawy. W dniu 29 kwietnia 2004 Minister SWiA wydał dwa rozporządzenia obowiązujące od 1 maja 2004 (dnia wejścia Polski do Unii Europejskiej) regulujące szczegółowo:

- dokumentację przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (opublikowane w Dz. U. z 2004 r. Nr 100, poz. 1024) - oznaczone w dalszym tekście jako rozporządzenie nr 1;
- wzór zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (opublikowane w Dz. U. z 2004 r. Nr 100, poz. 1025) - oznaczone w dalszym tekście jako rozporządzenie nr 2.

W myśl tych rozporządzeń wszystkie instytucje otrzymały pół roku na dostosowanie swoich rozwiązań organizacyjnych i procedur stosowanych w zarządzaniu do zapisów w nich opublikowanych. Ze względu na fakt, że wiele bibliotek bądź nie zrealizowało ich w całości, bądź jest dopiero na początku drogi, należy uporządkować wiedzę w tym zakresie.

W środowisku bibliotekarskim, a szczególnie w bibliotekach naukowych, konieczność podporządkowania się wymaganiom ustawy wzbudza do dnia dzisiejszego, jak sądzę niesłusznie, bardzo duże kontrowersje. Przesłanką, która stała się ich przyczyną jest art. 43 ust. 1 ustawy mówiący o tym, że administratorzy danych osobowych nie muszą rejestrować zbiorów danych przetwarzając je w związku z zatrudnieniem, świadczeniem usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się. Jeżeli zatem w bazie czytelników znajdują się tylko dane dotyczące studentów i pracowników własnej uczelni, zbiory takie nie podlegają rejestracji. Konieczność rejestracji z reguły wymusza okoliczność, że w bardzo niewielkim procencie czytelnikami są osoby z zewnątrz. Jak pokazują doświadczenia, powstanie takich kontrowersji jest nad wyraz inspirujące, bowiem określone tam wymagania inspirują zainteresowanie zarządzających sprawami bezpieczeństwa bibliotecznych systemów teleinformatycznych. Równocześnie skonkretyzowane i uporządkowane wymagania dotyczące bezpieczeństwa systemów komputerowych są podstawą zaprojektowania spójnego system ochrony zasobów. Zapobiega to typowemu działaniu służb informatycznych, polegającym na bezkrytycznym ograniczaniu funkcji dostępnych na stacjach roboczych.

Pierwszym etapem przygotowania i wdrożenia "firmowego" systemu bezpieczeństwa jest opracowanie "polityki bezpieczeństwa". Obowiązek ten wynika z artykułów nr 3 i 4 rozporządzenia nr 1. W polityce bezpieczeństwa zarządzający określa reguły i praktyczne zasady normujące sposób zarządzania, ochrony i rozpowszechniania informacji "produkowanej" w bibliotece. W zależności od stosowanej technologii informacje te mogą być gromadzone i przetwarzane w sposób tradycyjny (kartoteka papierowa) lub w systemach komputerowych. Zalecenia dotyczące tworzenia "polityki bezpieczeństwa" mówią, że powinna ona być: zatwierdzona przez dyrekcję biblioteki, oficjalnie opublikowana i dostępna na stałe dla pracowników. Ważne jest również to, że powinna ona deklarować pełne zaangażowanie kierownictwa w jej realizację. Minimalne wymagania wobec polityki bezpieczeństwa są określone w normie *PN-ISO 17799* z 2003 r. *Technika informatyczna - Praktyczne zasady zarządzania bezpieczeństwem informacji*.

W praktyce polityka ta powinna zawierać przynajmniej:

1. definicję bezpieczeństwa informacji, jej ogólne cele i zakres oddziaływania;
2. znaczenie bezpieczeństwa, jako mechanizmu umożliwiającego współużytkowanie informacji;
3. oświadczenie o intencjach kierownictwa zatwierdzające cele i zasady bezpieczeństwa informacji;
4. krótkie omówienie zasad, standardów i wymagań wymienionych w polityce bezpieczeństwa, a mających szczególne znaczenie dla instytucji. Przykładowo:
    - zgodność z prawem i wymaganiami wynikającymi z umów międzynarodowych lub firmowych;

- wymagania dotyczące kształcenia pracowników w zakresie przestrzegania zasad bezpieczeństwa (BARDZO WAŻNE);
- zapobieganie i wykrywanie wirusów oraz innego złośliwego oprogramowania zaburzającego pracę serwerów i stacji roboczych;
- zarządzanie ciągłością działania użytkowego instytucji;
- konsekwencje naruszenia polityki bezpieczeństwa;

5. definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji. W szczególności powinny zostać omówione zasady zgłaszania przypadków naruszenia bezpieczeństwa zasobów informacyjnych oraz działania podejmowane w reakcji na ich wystąpienie;
6. odsyłacze do innej, szczegółowej dokumentacji uzupełniającej politykę bezpieczeństwa tj.: szczegółowych polityk bezpieczeństwa pojedynczych systemów komputerowych, procedur postępowania przygotowanych dla całej instytucji lub systemów komputerowych oraz innych zasad bezpieczeństwa, które powinni przestrzegać pracownicy.

Ważne jest również, by sam dokument określający politykę bezpieczeństwa był napisany jasnym i konkretnym językiem o niskim poziomie abstrakcyjności, a przez to zrozumiałym dla wszystkich pracowników. Zasady postępowania omówione w polityce bezpieczeństwa powinny zawierać szczegółowe uzasadnienie przyjętych standardów i wymagań bezpieczeństwa. Jeżeli w naszej bibliotece przetwarzane są zarejestrowane zbiory danych osobowych, zgodnie z ustawą powinniśmy przygotować oddzielną politykę bezpieczeństwa dotyczącą tego zakresu. Powinna ona w całości wynikać z ogólnej polityki bezpieczeństwa biblioteki. Oczywiście ogólna polityka bezpieczeństwa biblioteki nie może stać w sprzeczności z polityką bezpieczeństwa jednostki nadrzędnej (dla nas - z polityką bezpieczeństwa Uniwersytetu Śląskiego).

Dla prawidłowego przygotowania i realizacji polityki bezpieczeństwa, tak ogólnej, jak i polityk szczegółowych, niezbędne jest dokonanie inwentaryzacji zasobów, które będą podlegać ich działaniu.

W związku z powyższym w art. 4 rozporządzenia w sposób szczegółowy wymieniono wszystkie składniki, które powinny zostać poddane inwentaryzacji. Są to głównie:

1. szczegółowy wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
2. szczegółowy wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
3. opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
4. sposób przepływu danych pomiędzy poszczególnymi systemami;
5. określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Ad.1
Ustawa w sposób szczegółowy definiuje istotę określenia "miejsce przetwarzania danych osobowych". Upraszczając, możemy powiedzieć że są to wszystkie pomieszczenia, gdzie je wprowadzamy, modyfikujemy, udostępniamy czy też je przechowujemy. Należy również pamiętać o wszystkich pomieszczeniach, gdzie mogą się one znaleźć, a w szczególności o szafach, zawierających papierowe archiwa z danymi osobowymi. Nie wolno zapominać także o miejscach, gdzie przechowujemy wycofany z eksploatacji lub uszkodzony sprzęt komputerowy. Zaliczają się do nich również miejsca, w których przechowujemy dobre lub uszkodzone elektroniczne nośniki danych, na których były przechowywane bazy danych osobowych (wymontowane dyski twarde, dyskietki od napędów ZIP, taśmy od streamerów, płyty optyczne CD i DVD). Jeżeli dane osobowe są przetwarzane równocześnie przez kilka bibliotek (np. wspólna baza czytelników), polityki bezpieczeństwa muszą być przygotowane oddzielnie dla każdej z nich. Równocześnie w polityce jednostki wiodącej powinny zostać wymienione wszystkie miejsca, gdzie są przetwarzane dane składowane we wspólnej bazie. W wykazie miejsc, gdzie przetwarzane są dane osobowe, powinny się również znaleźć lokalizacje serwerów zawierających bazy danych osobowych osób korzystających z możliwości zamawiania zbiorów poprzez OPAC.

Ad. 2
Podstawową sprawą przy identyfikacji przetwarzanych zbiorów informacji jest określenie nazw zbiorów oraz programów używanych do ich przetwarzania. W polityce bezpieczeństwa należy szczegółowo opisać strukturę oprogramowania używanego do przetwarzania zbioru danych osobowych, z uwzględnieniem sposobu jego instalowania, uaktualniania, konserwowania oraz administrowania uprawnieniami użytkowników. W przypadku oprogramowania składającego się z wielu modułów, należy określić szczegółowo granice ich oddziaływania oraz ewentualny wpływ zmian jednego modułu na pozostałe.

Ad. 3
W polityce bezpieczeństwa należy szczegółowo zdefiniować zawartość poszczególnych pól w rekordach gromadzonych danych osobowych oraz tych danych, które mogą mieć wpływ na przetwarzane dane osobowe. W szczególności należy zwrócić uwagę na te pola, które ze względu na swoją naturę (np. "uwagi o czytelniku") nie mają ściśle określonej zawartości. Dla takich pól polityka bezpieczeństwa powinna ściśle określać zakres informacji, które mogą zostać do niego wprowadzone. Należy również ustalić sposób weryfikacji raz wprowadzonych danych oraz sposób archiwowania poprawianej informacji. W szczególności należy określić, które pola powinny posiadać szczegółową historię zmian.

Ad. 4
Współczesne technologie informatyczne umożliwiają niemalże swobodne przekazywanie danych pomiędzy różnymi systemami informatycznymi, użytkowanymi w naszej instytucji (np. zintegrowany system obsługi studentów - dziekanatowy oraz zintegrowany system biblioteczny). Dla takich rozwiązań polityka bezpieczeństwa musi ściśle zdefiniować akceptowane przez nas kanały dystrybucji informacji. Powinien zostać zdefiniowany maksymalny zakres dystrybuowanych danych oraz cel ich przekazywania. W przypadku bibliotek mogą to być wykazy nierzetelnych czytelników, przekazywanych wzajemnie przez biblioteki rejestrujące wypożyczenia książek w sposób rozproszony w różnych systemach komputerowych lub identyczne wykazy przekazywane do dziekanatów. System musi umożliwiać rejestrowanie w sposób trwały zakresu przekazanych danych. Równocześnie należy określić zestaw danych, który może podlegać automatycznej aktualizacji. W przypadku sieci bibliotek uczelni wyższych mogą to być adresy korespondencyjne używane w chwili wysyłania upomnień. Dane te mogą być automatycznie aktualizowane z systemu kadrowego dla upomnień pracowniczych oraz dziekanatowego dla upomnień wysyłanych do studentów.

Ad. 5
Element ten jest bardzo ważny i ulega niestety najczęstszym zmianom. Opisuje on w sposób zwięzły, jasny i ścisły wszystkie działania podejmowane przez służby informatyczne dla zapewnienia poufności gromadzonych danych osobowych. Określa on również zakres niezbędnych działań podjętych wobec pracowników poprzez zdefiniowanie ich roli w zakresie przestrzegania przyjętych zasad. Z reguły w polityce określa się podstawowe normy postępowania. Ze względu na gwałtowny rozwój systemów operacyjnych stacji roboczych oraz systemów operacyjnych i motorów baz danych instalowanych na serwerach, szczegółowe rozwiązania powinny zostać określone dopiero w załącznikach do polityki. Załączniki te winny być aktualizowane przy każdej zmianie stosowanej technologii informatycznej. O zaistnieniu takiej sytuacji powinni zostać w sposób jawny powiadomieni wszyscy pracownicy, których taka zmiana dotyczy. Dla zapewnienia stabilności ochrony systemów główna polityka bezpieczeństwa firmy powinna być zmieniana tylko w ostateczności, gdy już nie ma możliwości załatwienia tej sprawy poprzez odpowiednie załączniki. Szczegółowy zakres elementów związanych z bezpieczeństwem zostanie omówiony w dalszej części opracowania.

Na podstawie założeń zdefiniowanych w polityce bezpieczeństwa administrator danych osobowych (kierownik jednostki - dyrektor biblioteki) zobowiązany jest do przygotowania instrukcji określającej sposób zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji. Instrukcja lub instrukcje takie powinny zostać zatwierdzone przez administratora danych osobowych do stosowania, a zawarte w nich zapisy przekazane do realizacji przez pracowników.

W instrukcji powinny zostać zawarte ogólne informacje o systemie informatycznym i zbiorach danych osobowych, które są przy ich użyciu przetwarzane. Omawiamy tam również wdrożone rozwiązania techniczne, procedury eksploatacji oraz zasady użytkowania sprzętu i systemów zastosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Jeżeli w bibliotece do przetwarzania danych osobowych wykorzystujemy kilka systemów informatycznych lub inne systemy mogą wpływać na system podstawowy, instrukcja taka może dotyczyć wszystkich systemów naraz lub można dla każdego z nich opracować ją oddzielnie.

W minimalnej postaci instrukcja taka musi obejmować elementy określone w art. 5 rozporządzenia, tj.:

1. procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2. stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
3. procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
4. procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
5. sposób, miejsce i okres przechowywania:
    - elektronicznych nośników informacji zawierających dane osobowe;
    - kopii zapasowych, o których mowa w pkt. 4;
6. sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania umożliwiającego nieuprawniony dostęp do systemu informatycznego;
7. sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia, tj. informacji o odbiorcach gromadzonych przez nas danych osobowych;
8. procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Dla zapewniania ochrony przetwarzanych danych osobowych w minimalnym zakresie instrukcja powinna określać szczegółowe zasady postępowania w każdym z wymienionych powyżej działów.

Ad. 1
Należy tutaj zdefiniować zasady przyznawania użytkownikowi identyfikatora (lub w przypadku takiej potrzeby identyfikatorów) w systemie informatycznym, jak również zasady nadawania lub modyfikacji uprawnień użytkownika do zasobów systemu informatycznego. Powinny one obejmować operacje związane z nadawaniem użytkownikom uprawnień począwszy od utworzenia użytkownikowi konta, poprzez przydzielanie i modyfikację jego uprawnień, aż do momentu usunięcia konta z systemu informatycznego. Jesteśmy tutaj zobowiązani do określenia w sposób jednoznaczny zasad postępowania z hasłami użytkowników oraz administratorów systemów informatycznych, a także procedur postępowania w przypadku pozyskania haseł przez osoby nieuprawnione. Definiujemy również zasady administrowania systemem informatycznym w przypadkach awaryjnych, np. nieobecności odpowiedniego administratora.

Ad. 2
Należy tutaj określić tryb przydzielania haseł. Trzeba opisać, czy hasła mają być przekazywane użytkownikom w formie ustnej, czy pisemnej oraz opisać stopień jego złożoności. W zależności od sposobu przyłączenia do sieci określono minimalną długość haseł, zakres używanych znaków (małe i duże litery, cyfry i znaki specjalne), minimalną częstotliwość jego zmiany oraz ilość zapamiętywanych przez system haseł. Należy również określić osoby upoważnione do zmiany haseł na żądanie użytkowników (osobowe lub funkcjonalne). Niedopuszczalne jest przekazywanie nazw użytkowników oraz haseł poprzez osoby trzecie lub za pośrednictwem niechronionych wiadomości poczty elektronicznej. W zależności od zastosowanego systemu możemy wymusić przy pierwszym logowaniu konieczność zmiany hasła. Rozporządzenie szczegółowo określa zasady tworzenia haseł: hasło użytkownika powinno być zmieniane nie rzadziej niż co 30 dni i składać się co najmniej z 6 znaków, jeżeli w systemie nie są przetwarzane dane,

o których mowa w art. 27 ustawy lub 8 znaków, jeżeli takie dane są przetwarzane. Hasła w systemie informatycznym powinny być przechowywane w postaci zaszyfrowanej. Należy również opisać sposób przechowywania haseł administratorów i ewidencji awaryjnego ich używania następującego po otwarciu (pierwotnie zamkniętych) zdeponowanych w szafach ognioodpornych kopert.

Ad. 3
W punkcie tym należy wyspecyfikować kolejne czynności wykonywane podczas uruchamiania systemu informatycznego przetwarzającego dane osobowe. Bardzo szczegółowo należy opisać wszystkie czynności i zasady postępowania użytkowników podczas przeprowadzania procesu uwierzytelniania się (logowania się do systemu). Instrukcja powinna określać sposoby postępowania użytkowników mające na celu zachowanie poufności haseł oraz uniemożliwiać nieuprawnione przetwarzanie danych. Należy również określić metody postępowania w sytuacji tymczasowego zawieszenia pracy, następującego na skutek chwilowego opuszczenia stanowiska pracy lub w okolicznościach, kiedy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba. Instrukcja powinna określać sposoby informowania użytkowników o ich powinnościach w chwili zaprzestania pracy, poprzez opisanie sposobów wylogowywania się z systemu oraz wyłączania stacji roboczej. Procedury przeznaczone dla użytkowników systemów przetwarzających dane osobowe w sposób jednoznaczny muszą określać sposób postępowania w sytuacji podejrzenia naruszenia bezpieczeństwa systemu, np. braku możliwości zalogowania się użytkownika na jego konto, zauważenia zmiany zawartości danych lub innych symptomów, wskazujących na ingerencję osób nieuprawnionych w przetwarzane dane lub użytkowany sprzęt.

Ad. 4
Należy tutaj opisać sposób i częstotliwość tworzenia zapasowych kopii danych przetwarzanych w systemie oraz kopii samego oprogramowania używanego do ich przetwarzania. Szczegółowo określamy rodzaj zabezpieczanych danych, nośnik na którym będziemy je zabezpieczać, narzędzia programowe, którymi będziemy się posługiwać oraz sprzętu, na którym będziemy pracować. W procedurze określamy dokładny harmonogram wykonywania kopii zapasowych dla poszczególnych zbiorów danych wraz ze wskazaniem wybranej metody sporządzania kopii (kopia przyrostowa, kopia całościowa). Jeżeli procedura wykonywania kopii jest bardzo skomplikowana, możemy opisać ją jako zestaw procedur odwołujący się do poszczególnych systemów. W takim przypadku szczegółowe procedury są załączone do instrukcji zarządzania systemami. W procedurach opisujących wykonywanie kopii zapasowych określamy maksymalny czas używania poszczególnych nośników, sposób ich rotacji oraz sposoby ich likwidacji. Procedura likwidacji nośników zawierających dane osobowe powinna uwzględniać wymogi zawarte w załączniku do rozporządzenia, nakazujące by wszystkie urządzenia (dyski twarde lub inne nośniki elektroniczne) zawierające dane osobowe, przeznaczone do wymiany gwarancyjnej lub likwidacji, pozbawiać zapisu tych danych, a gdy nie jest to możliwe, uszkadzać w sposób uniemożliwiający ich odczytanie. Przykładowo dla dysków twardych może być to przeprowadzane poprzez wymontowanie z ich obudowy talerzy z nośnikiem magnetycznym i zniszczeniu ich przy pomocy prasy hydraulicznej o odpowiednio dużej sile nacisku, powodującej całkowite zniszczenie mechaniczne.

Ad. 5.
Należy tutaj opisać sposób i czas przechowywania nośników informacji używanych do wykonywania kopii zapasowych (taśmy magnetyczne, płyty optyczne CD i DVD oraz dyskietki FDD i ZIP). Określeniu podlegają również pomieszczenia, przeznaczone do przechowywania nośników informacji, jak również sposoby fizycznego i logicznego zabezpieczenia przed nieuprawnionym przejęciem, odczytem, skopiowaniem oraz zniszczeniem (szafy metalowe, ogniotrwałe, deponowanie na zewnątrz). Przy opracowywaniu zaleceń uwzględniamy wymogi załącznika do rozporządzenia (pkt 4 ppkt 4a). W czasie przygotowania instrukcji należy pamiętać, że kopie awaryjne należy usuwać bezzwłocznie po ustaniu ich użyteczności. Jeżeli podejmujemy decyzję o przechowywaniu kopii zapasowych na zewnątrz, należy szczegółowo określić procedury bezpiecznego ich deponowania uwzględniające również czas ich transportu.

Ad. 6
W punkcie tym należy zdefiniować obszary użytkowanych przez nas systemów narażone

na ingerencję wirusów komputerowych oraz wszelkiego innego rodzaju oprogramowania mogącego mieć wpływ na bezpieczeństwo przetwarzanych danych osobowych. Należy określić wszelkie możliwe do zidentyfikowania źródła przedostawania się szkodliwego oprogramowania do serwerów lub stacji roboczych oraz działania, jakie będą podejmowane, by zminimalizować możliwość zainstalowania takiego oprogramowania na naszych komputerach. Instrukcja powinna zawierać specyfikację stosowanego oprogramowania przeciwdziałającego szkodliwemu działaniu oprogramowań "wrogich". Należy wyspecyfikować nazwy oprogramowań antywirusowych stosowanych w firmie oraz określić sposób i częstotliwość uaktualniania bazy wirusów. Użytkownik musi zostać przeszkolony w zakresie procedur postępowania w przypadku, gdy oprogramowanie zabezpieczające wskazuje zaistnienie zagrożenia. W punkcie tym należy również wyspecyfikować wszystkie inne sposoby zabezpieczające nasze serwery i stacje robocze przed nieuprawnionym pozyskiwaniem danych osobowych. Mogą do nich należeć np. fizyczne blokady urządzeń zapisujących dane na nośnikach wymiennych (streamery, stacje optyczne z funkcją zapisu czy stacje FDD i ZIP).

Ad. 7.
Jest to punkt, który będzie w praktyce dotyczył znikomej liczby bibliotek. Z reguły w naszej działalności statutowej dane osobowe są gromadzone na potrzeby własne. Jedynym wyjątkiem może być przekazywanie danych osobowych czytelników zalegających ze zwrotem książek instytucjom, które mogą mieć wpływ na przyspieszenie ich zwrotu. Przykładowo może być to wykaz studentów danej uczelni, którzy nie zwrócili książek do bibliotek pedagogicznych lub publicznych. Biblioteki, które chcą w sposób formalny wykorzystywać takie możliwości powinny informacje o stosowaniu takich procedur zawrzeć w swoich regulaminach oraz deklaracjach, w których w sposób jawny lub poprzez odniesienie do regulaminu, w którym czytelnik akceptuje takie rozwiązania formalne.

Ad. 8.
Należy tutaj określić zakres, częstotliwość oraz procedury wykonywania przeglądów i konserwacji systemu informatycznego. Dotyczy to w równej mierze sprzętu, jak i oprogramowania. Należy wskazać firmy i osoby fizyczne niebędące naszymi pracownikami, uprawnione do dokonywania przeglądów i konserwacji systemu oraz zakres prac wykraczający poza normalne działanie systemu (np. bezpośrednie blokady danych wykonywane w motorze bazy danych w celu uzupełnienia nieistniejących funkcjonalności w systemie bibliotecznym) mogące mieć wpływ na bezpieczeństwo danych osobowych poprzez naruszenie integralności bazy danych. Procedury wykonywania czynności konserwacyjnych zlecane osobom niemającym uprawnień do przetwarzania danych (np. firmom zewnętrznym), winny określać sposób nadzorowania przez administratora danych wykonywanych prac oraz określać sposoby niedopuszczenia do nieuprawnionego pozyskiwania danych.

Po przygotowaniu polityki bezpieczeństwa i instrukcji określającej sposób zarządzania systemami informatycznymi prostym jest już wypełnienie *Zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych*. Zawiera on informacje formalne podawane w częściach od A do D oraz część E opisującą konfigurację systemu przetwarzającego dane osobowe oraz wszystkie środki bezpieczeństwa podjęte przez instytucję w celu uniemożliwienia nieuprawnionego dostępu do danych. Źródłem danych do przygotowania zgłoszenia są w prostej linii opracowana przez nas polityka bezpieczeństwa oraz uzupełniające ją odpowiednie instrukcje.

Scharakteryzowane powyżej czynności, oprócz wypełnienia warunków formalnych, są okazją do uporządkowania organizacyjnego naszej instytucji. Zapobiegają również stosowaniu rozwiązań nadmiarowych i zbędnych, utrudniających lub uniemożliwiających w sposób oczywisty pracę biblioteki i mogą stać się wstępem do prac zmierzających do uzyskania certyfikatu ISO 9000.

W przypadku zainteresowania rozwiązaniami szczegółowymi BUŚ zapraszam do kontaktów bezpośrednich, bo tylko takie są dopuszczalne prawnie.

Bibliografia

1. Mitnick, K.D., *Sztuka podstępu: łamałem ludzi nie hasła*, Gliwice: Helion 2003. ISBN 83-7361-108-8.

2. *PN-ISO/IEC 17799:2003 Technika informatyczna - Praktyczne zasady zarządzania bezpieczeństwem informacji.*

3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. *Dziennik Ustaw* 2004 r. nr 100, poz. 1024.

4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. *Dziennik Ustaw* 2004 r. nr 100, poz. 1025.

5. *Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych*, z późniejszymi zmianami, tekst jednolity. *Dziennik Ustaw* 2002 r. nr 101 poz. 926.

Prace nad wdrożeniem procedur zabezpieczających przestrzeganie Ustawy o Ochronie Danych Osobowych oraz związanych z nią rozporządzeń wykonawczych / Andrzej Koziara// W: Biuletyn EBIB [Dokument elektroniczny] / red. naczelny Bożena Bednarek-Michalska. - Nr 5/2005 (66) maj. - Czasopismo elektroniczne. - [Warszawa] : Stowarzyszenie Bibliotekarzy Polskich KWE, 2005. - Tryb dostępu: http://www.ebib.pl/2005/66/koziara.php. - Tyt. z pierwszego ekranu. - ISSN 1507-7187